実対処から見える保全の阻害要因

セコムトラストシステムズ株式会社
2014年11月20日

アジェンダ

- はじめに
- HDDデータ保全時の阻害要因
  - 調査の全体像
  - 阻害要因１，２，３
  - 痕跡不足の具体例
  - 対策案
- 物理メモリデータ保全における痕跡消失
  - 痕跡の消失例
  - 注意点
- 対策案まとめ

はじめに

会社紹介

Total Information Service

セコムトラストシステムズ株式会社

Secom Trust Systems Co.,Ltd.（略称:STS）

■設立 ：1985年（昭和60年）8月
■代表者 ：代表取締役社長　泉田 達也
■年間売上高 ：323億円（2014年3月期）
■社員数 ：912名(2014年3月31日現在)
■資本金 ：14億6,880万円

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ㈱

➢情報セキュリティと大規模災害対策をコアとしたトータル情報サービス会社

➢ITをうまく活用して便利・快適・効率化を進めるとともに、あらゆる「不安」の無い社会実現を目指します

セコムプロフェッショナルサポート Total Information Service

お客様の緊急事態にセキュリティのプロとして駆けつけ、事業継続、事業復旧を強力にサポートします。

対象インシデント	・ウイルス感染 ・不正アクセス ・WEB改ざん
作業例	・ウイルス駆除、ウイルス感染調査 ・不正アクセス調査 ・社内ポリシー違反に関する調査 ・WEB改ざんインシデント対応支援等
特徴	お客様に生じた業務の混乱や停止からの早期復旧に向け、お客様先に駆けつけることを重視しています。

サイバー消防団

HDDデータ保全時の阻害要因

調査の全体像

Total Information Service

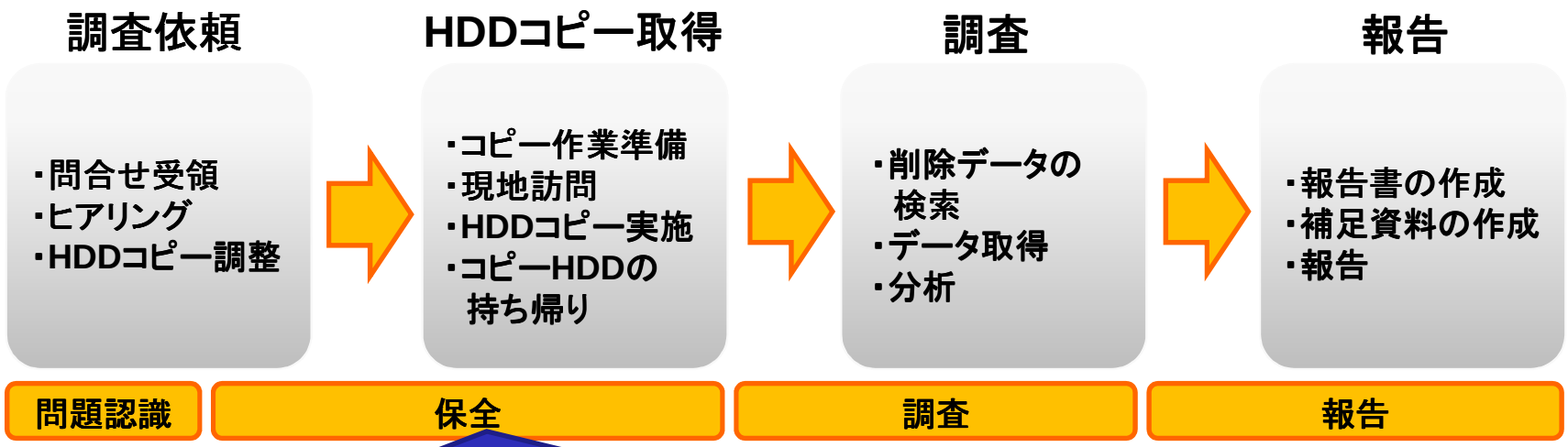
調査依頼	HDDコピー取得	調査	報告
・問合せ受領 ・ヒアリング ・HDDコピー調整	・コピー作業準備 ・現地訪問 ・HDDコピー実施 ・コピーHDDの持ち帰り	・削除データの検索 ・データ取得 ・分析	・報告書の作成 ・補足資料の作成 ・報告

■調査目的

【サイバー攻撃調査】
- ・ウイルス感染有無の調査
- ・ウイルス感染原因の調査
- ・ウイルス感染影響の調査

【社内ポリシー違反】
- ・USBメモリ接続有無の調査
- ・アプリケーション導入有無の調査
- ・掲示板サイトへのアクセス有無調査

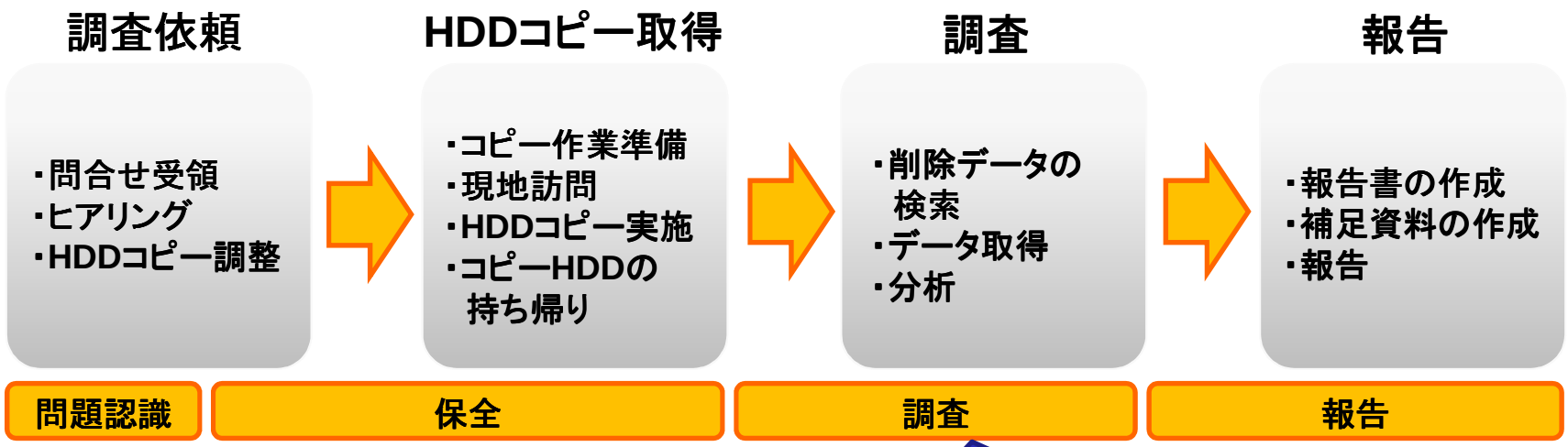
保全の阻害要因1



■保全時に気がつく保全の阻害要因

・HDDインタフェースの違い（SATA、IDE、SCSI、SAS）
⇒作業の再調整
・HDD容量の違い
⇒作業の再調整、作業時間の延長
・HDDの故障
⇒物理サルベージの実施、調査対象外とする
・ATAパスワードロック
⇒パスワード解除作業

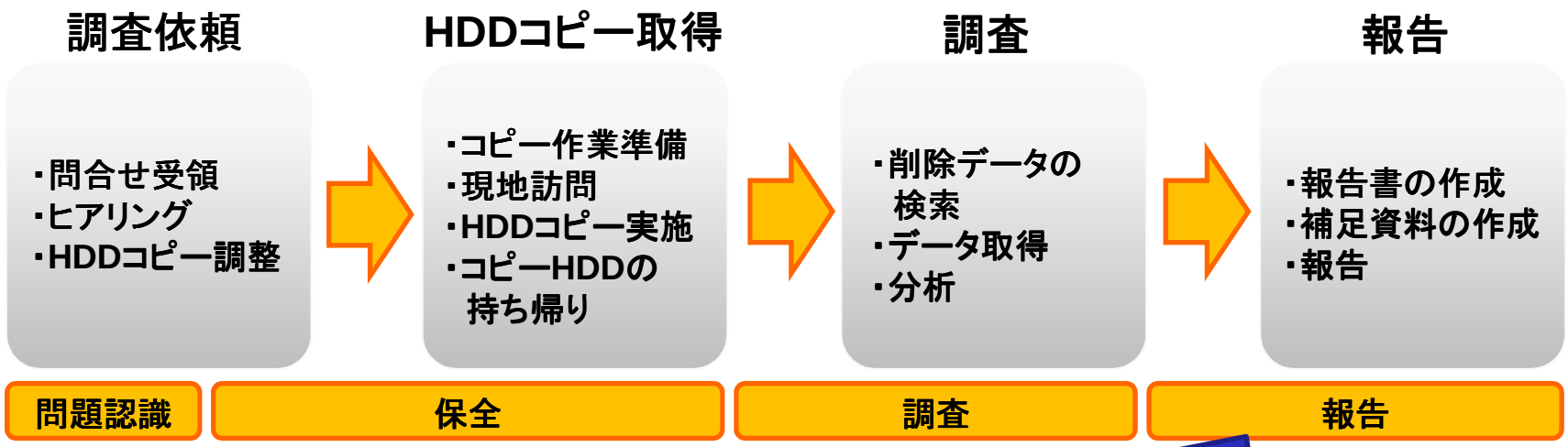
保全の阻害要因2



■調査時に気づく保全の阻害要因

・HDDが暗号化されている
⇒暗号化の解除、HDDコピーの再取得
・対象が完全に初期化されている
⇒調査ができない

保全の阻害要因3



■結果的な保全の阻害要因

・痕跡不足
⇒期待した結果（ウイルスの感染原因など）を得られない

【原因】
・問題認識後、第一にウイルス駆除を実施している
・該当端末を使用(業務利用)し続けている
・業務データ取得のために、該当端末の起動・停止を繰り返している

痕跡が消える
認識が薄い

痕跡不足の具体例

プログラム実行履歴の痕跡例

＜問合せの受付＞
6月24日
＜依頼＞
PCが6/17以前にウイルスに感染していた形跡があるため、ウイルスの感染原因を知りたい
＜保全までのPC状態＞
・6月17日にウイルス駆除作業を実施
・6月27日まで通常業務に利用

■プログラム実行履歴例

実行日時	実行ファイル	ファイルパス	回数
2014/6/27 11:39:18	LOGONUI.EXE	C:¥WINDOWS¥SYSTEM32¥LOGONUI.EXE	46
2014/6/27 11:39:17	RUNDLL32.EXE	C:¥WINDOWS¥SYSTEM32¥RUNDLL32.EXE	11
2014/6/27 11:39:08	ADOBE CEF HELPER.EXE	C:¥PROGRAM FILES (X86)¥ADOBE¥ADOBE CREATIVE CLOUD¥HEX¥ADOBE CEF HELPER.EXE	74
2014/6/27 11:39:05	IGFXSRVC.EXE	C:¥WINDOWS¥SYSTEM32¥IGFXSRVC.EXE	588
2014/6/27 11:37:47	SEARCHFILTERHOST.EXE	C:¥WINDOWS¥SYSTEM32¥SEARCHFILTERHOST.EXE	793

・調査に必要な6月17日以前の履歴が少ない
⇒全164件中、6/17以前の履歴が32件、6/17以降の履歴が132件

対策案

◆HDDインタフェースの違い
⇒様々なインタフェースに対応できる準備

◆HDD容量の違い
⇒容量変化に対応できる準備

◆HDDの故障
⇒長く放置されている場合には故障の可能性も頭の片隅に

◆ATAパスワードロック
⇒パスワードロック実施の把握

◆HDDが暗号化されている
⇒HDD暗号化の把握、コピー取得後早めのHDDアクセス

◆対象が完全に初期化されている
⇒端末押収時に注意

◆痕跡不足
⇒調査を見据えた、インシデント時の体制・フローの確立

物理メモリデータ保全における痕跡消失

Secom Trust Systems Co.,Ltd.
信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

痕跡の消失例と注意点

■LAN線の抜線

・LAN線が抜かれたことで動作を変える(停止する)ウイルス

■ウイルススキャン

・ウイルス対策ソフトのスキャンによる物理メモリデータの消失

スキャン前のメモリダンプ(通信情報)

Offset(P)	Local Address	Remote Address	Pid
0x015f38a8	192.168.1.89:1086	232.44.251:80	2652
0x01608008	192.168.1.89:1063	106.108.6:80	2652
0x01649308	192.168.1.89:1035	44.149.163:80	160
0x01678548	64.0.0.0:38785	.0.0:20606	2171045216
0x01755008	192.168.1.89:1082	.232.238.6:80	2652
0x01756790	192.168.1.89:1078	.194.117.184:80	2652
0x0175ba28	192.168.1.89:1109	.168.1.200:139	0
0x01b2b880	192.168.1.89:1064	.194.117.186:80	36700164
0x0352d548	64.0.0.0:38785	.0.0:20606	2171045216
0x04a25008	192.168.1.89:1063	106.108.6:80	2652
0x04b94548	64.0.0.0:38785	.0.0:20606	2171045216

メモリダンプ上に
残る履歴の減少

スキャン後のメモリダンプ(通信情報)

Offset(P)	Local Address	Remote Address	Pid
0x015f38a8	0.0.0.0:0	.0.0:0	3134238896
0x01608008	192.168.1.89:1063	106.108.6:80	2652
0x01649308	1.0.0.0:0	116.70.115:0	0
0x01678548	3.0.49.2:28129	.0.0:21349	0
0x01755008	192.168.1.89:1082	.232.238.6:80	2652
0x01756790	192.168.1.89:1078	.194.117.184:80	2652
0x0175ba28	192.168.1.89:1113	.168.1.232:8080	432
0x017e79a0	40.65.85.129:38017	116.102.114:8233	0

注意点

- LAN線の抜線やウイルス対策ソフトによるスキャンにより、痕跡の消える可能性があることを、まず認識する。

- LAN線を抜く、ウイルス対策ソフトによるスキャンより前に保全を実施することで、少しでも多くの痕跡残が期待できる。

対策案まとめ

- インシデントの発生を想定した準備が大切

- インシデント発生時の体制の構築、フローの確立
  - 発生するインシデントの想定
  - 意志決定者、関係者が決まっているか
  - 意志決定者を含む関係者への情報伝達スキーム
  - 意志決定を受けて行動するのは誰か

ご清聴ありがとうございました。